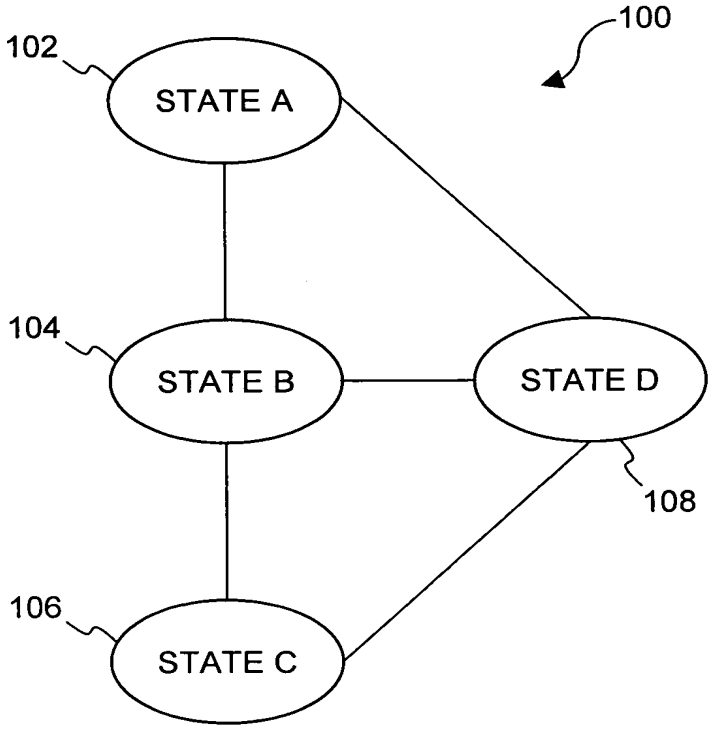


FIG. 1

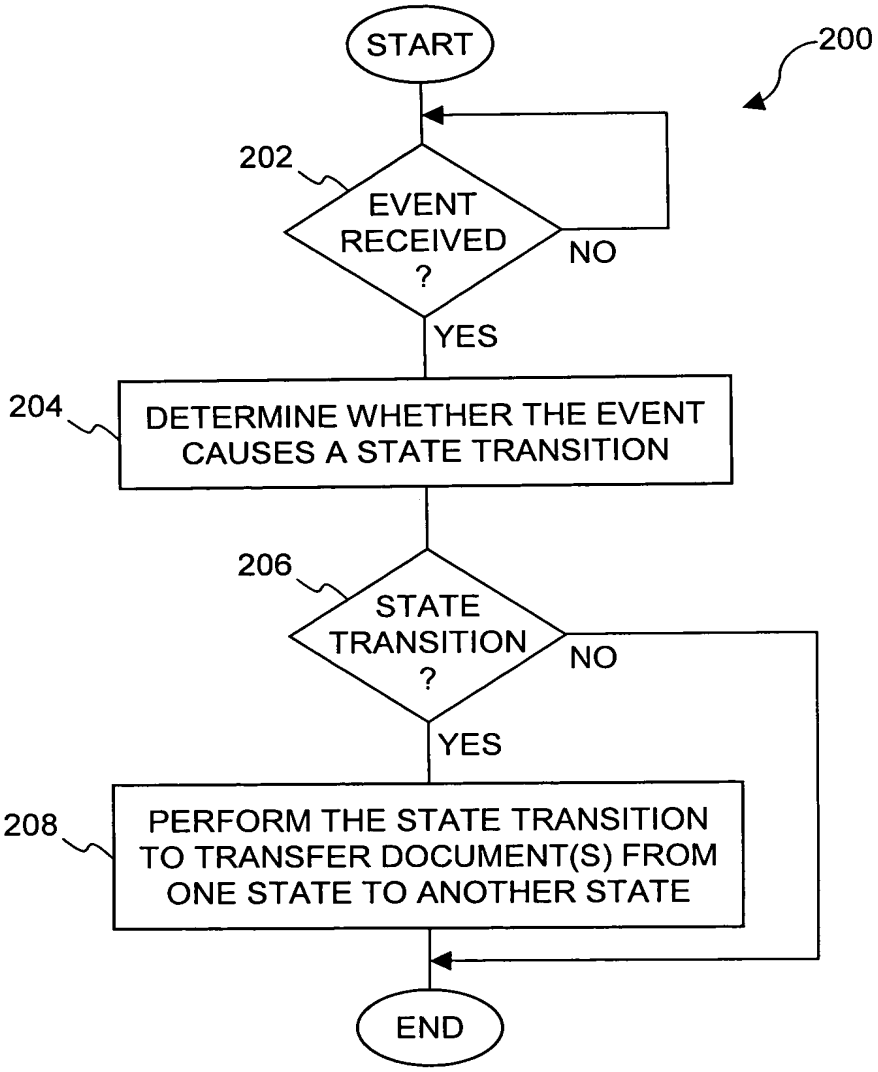
START
200
202
EVENT RECEIVED ?
NO
YES
204
DETERMINE WHETHER THE EVENT CAUSES A STATE TRANSITION
206
STATE TRANSITION ?
NO
YES
208
PERFORM THE STATE TRANSITION TO TRANSFER DOCUMENT(S) FROM ONE STATE TO ANOTHER STATE
END

FIG. 2

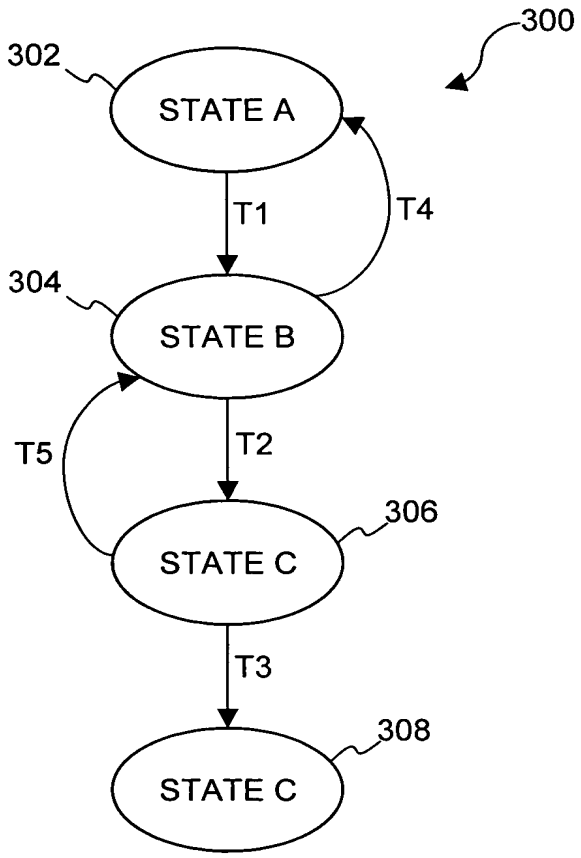


FIG. 3

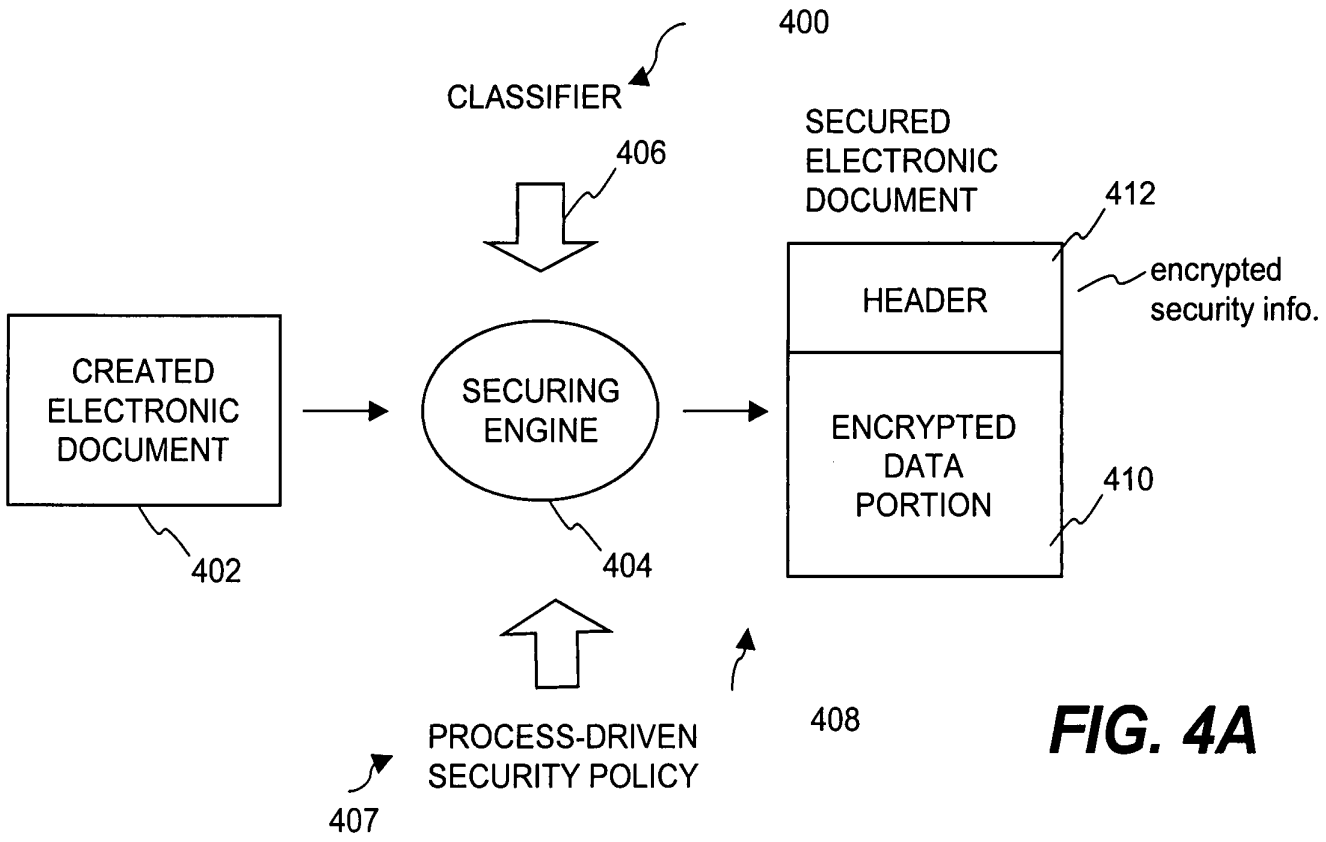
400
CLASSIFIER
406
SECURED
ELECTRONIC
DOCUMENT
412
HEADER
encrypted
security info.
CREATED
ELECTRONIC
DOCUMENT
SECURING
ENGINE
ENCRYPTED
DATA
PORTION
410
402
404
408
PROCESS-DRIVEN
SECURITY POLICY
407

FIG. 4A

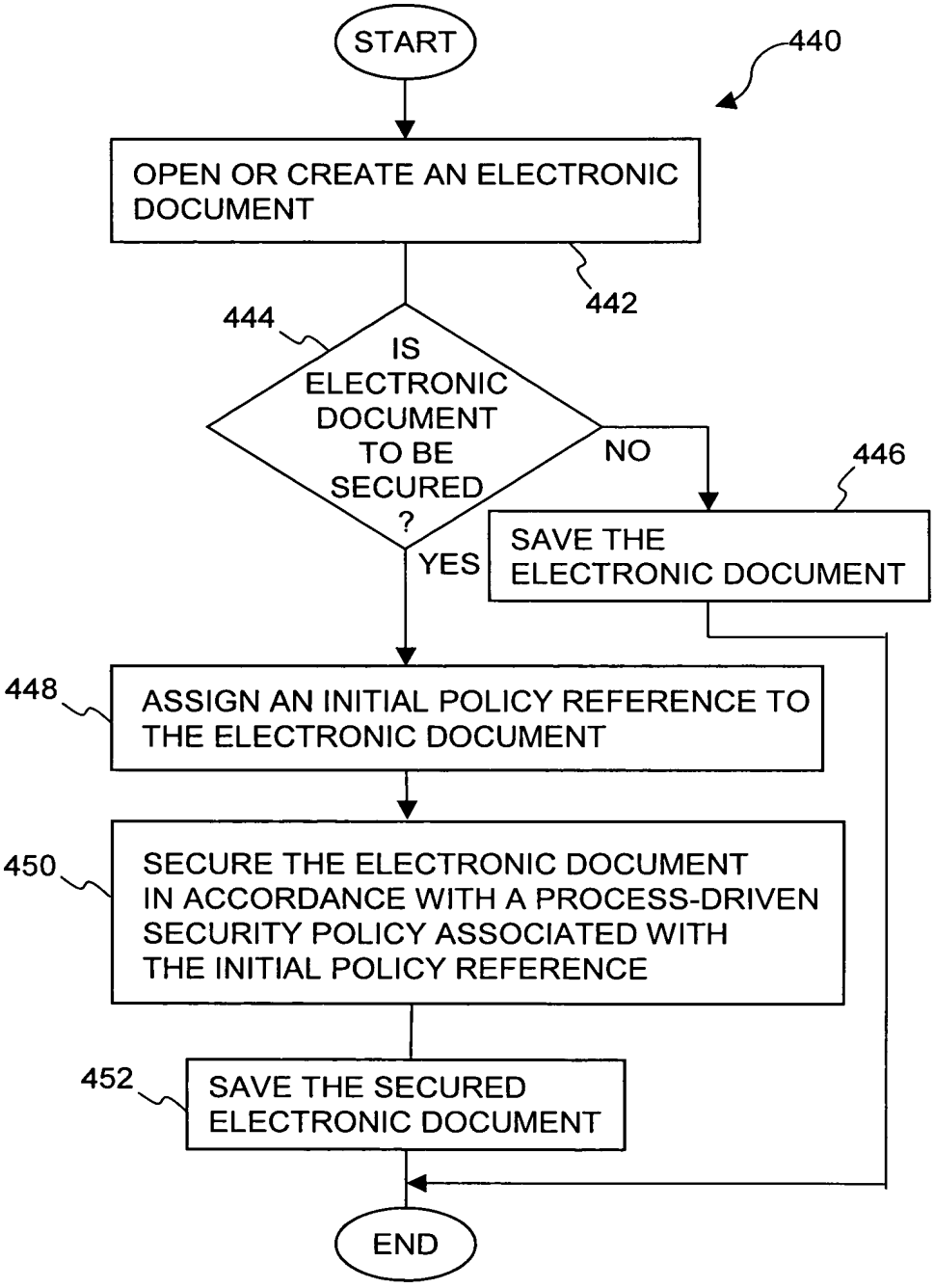
START
440
OPEN OR CREATE AN ELECTRONIC DOCUMENT
442
444
IS ELECTRONIC DOCUMENT TO BE SECURED ?
NO
446
SAVE THE ELECTRONIC DOCUMENT
YES
448
ASSIGN AN INITIAL POLICY REFERENCE TO THE ELECTRONIC DOCUMENT
450
SECURE THE ELECTRONIC DOCUMENT IN ACCORDANCE WITH A PROCESS-DRIVEN SECURITY POLICY ASSOCIATED WITH THE INITIAL POLICY REFERENCE
452
SAVE THE SECURED ELECTRONIC DOCUMENT
END

FIG. 4B

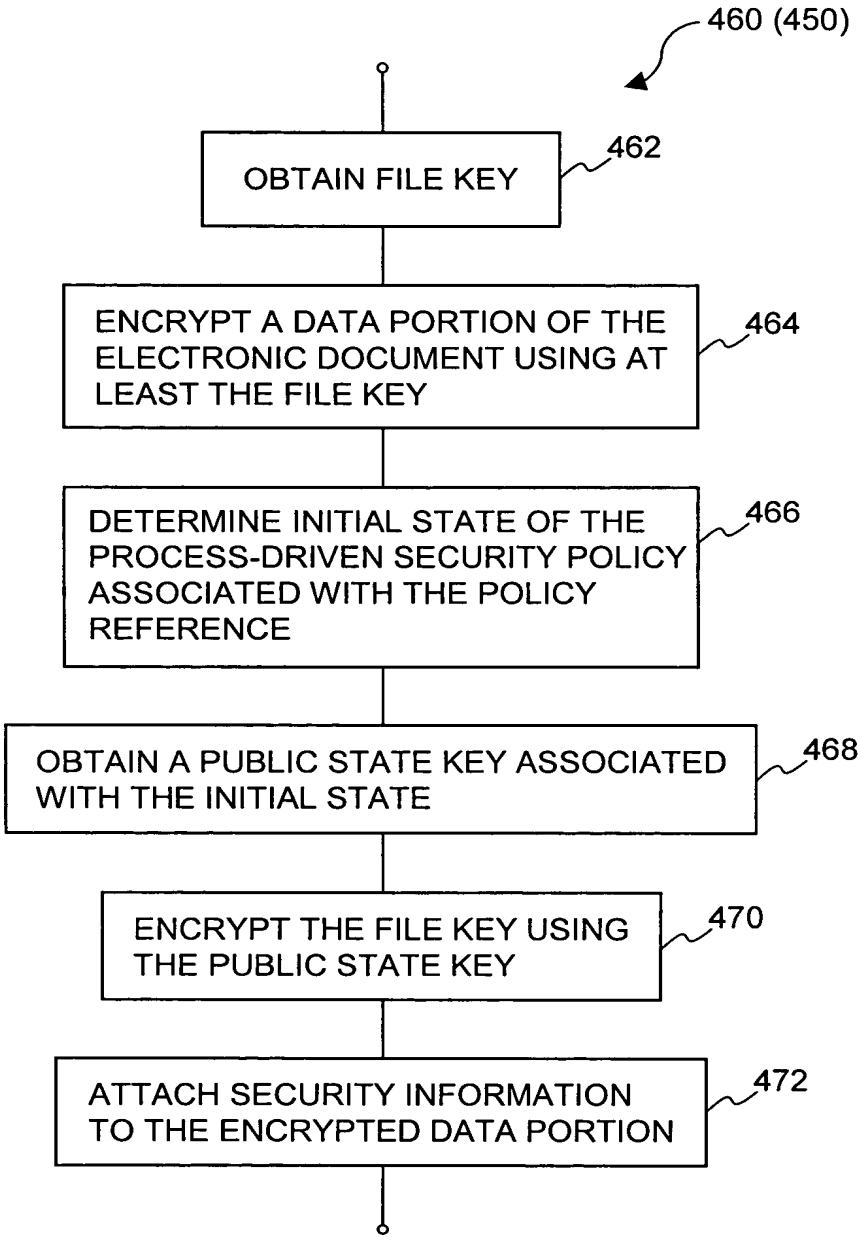
460 (450)
OBTAIN FILE KEY
462
ENCRYPT A DATA PORTION OF THE ELECTRONIC DOCUMENT USING AT LEAST THE FILE KEY
464
DETERMINE INITIAL STATE OF THE PROCESS-DRIVEN SECURITY POLICY ASSOCIATED WITH THE POLICY REFERENCE
466
OBTAIN A PUBLIC STATE KEY ASSOCIATED WITH THE INITIAL STATE
468
ENCRYPT THE FILE KEY USING THE PUBLIC STATE KEY
470
ATTACH SECURITY INFORMATION TO THE ENCRYPTED DATA PORTION
472

FIG. 4C

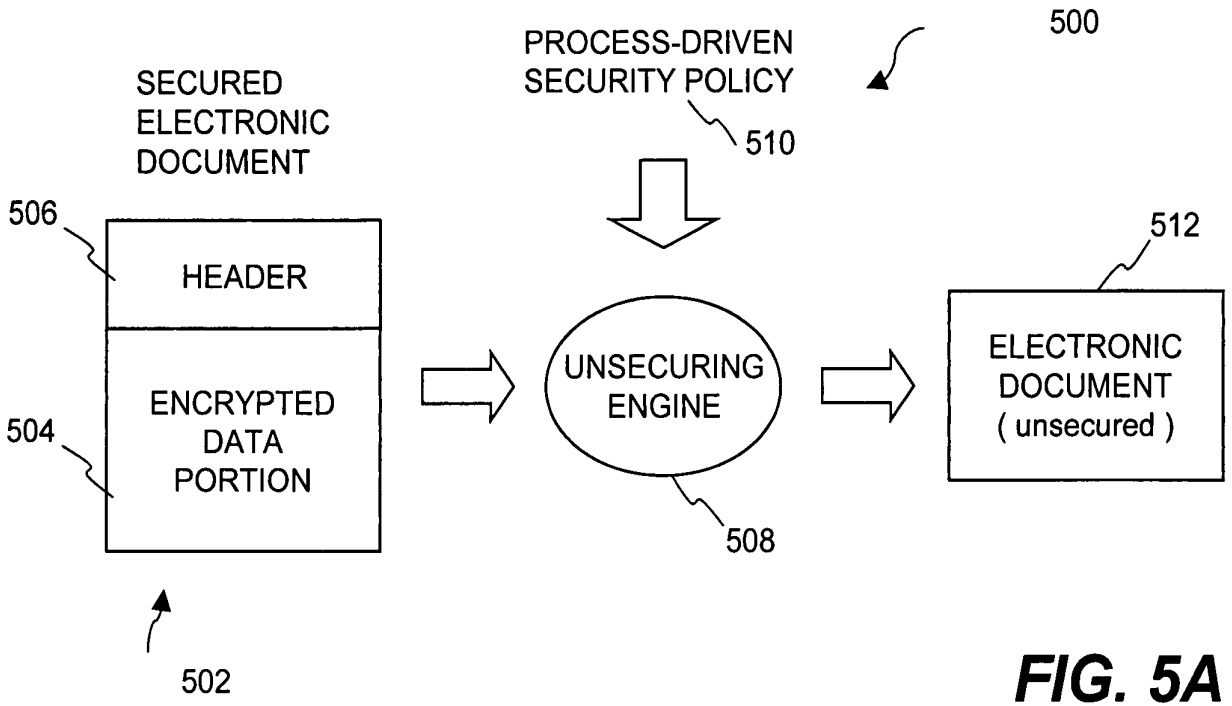
500
PROCESS-DRIVEN
SECURITY POLICY
510
SECURED
ELECTRONIC
DOCUMENT
506
HEADER
504
ENCRYPTED
DATA
PORTION
502
UNSECURING
ENGINE
508
512
ELECTRONIC
DOCUMENT
( unsecured )

FIG. 5A

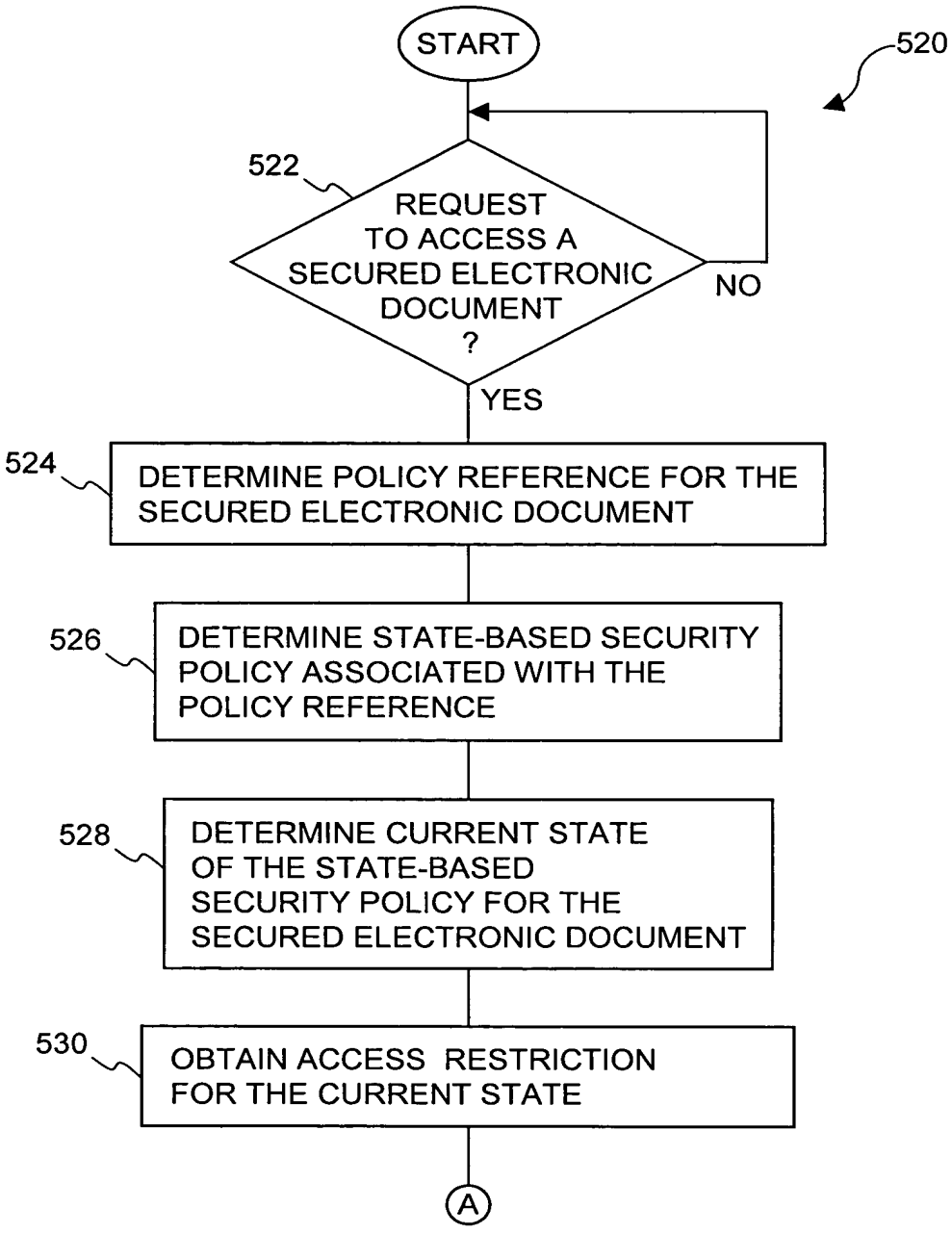
START
520
522
REQUEST TO ACCESS A SECURED ELECTRONIC DOCUMENT ?
NO
YES
524
DETERMINE POLICY REFERENCE FOR THE SECURED ELECTRONIC DOCUMENT
526
DETERMINE STATE-BASED SECURITY POLICY ASSOCIATED WITH THE POLICY REFERENCE
528
DETERMINE CURRENT STATE OF THE STATE-BASED SECURITY POLICY FOR THE SECURED ELECTRONIC DOCUMENT
530
OBTAIN ACCESS RESTRICTION FOR THE CURRENT STATE
A

FIG. 5B

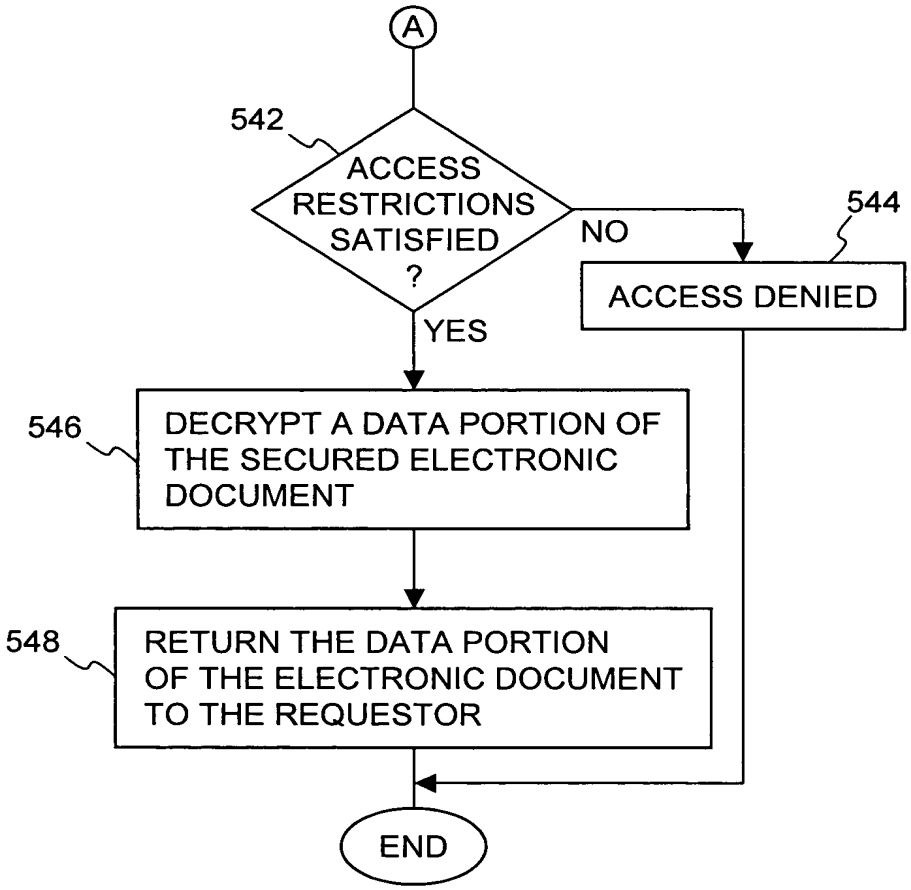
A
542
ACCESS RESTRICTIONS SATISFIED ?
NO
544
ACCESS DENIED
YES
546
DECRYPT A DATA PORTION OF THE SECURED ELECTRONIC DOCUMENT
548
RETURN THE DATA PORTION OF THE ELECTRONIC DOCUMENT TO THE REQUESTOR
END

FIG. 5C

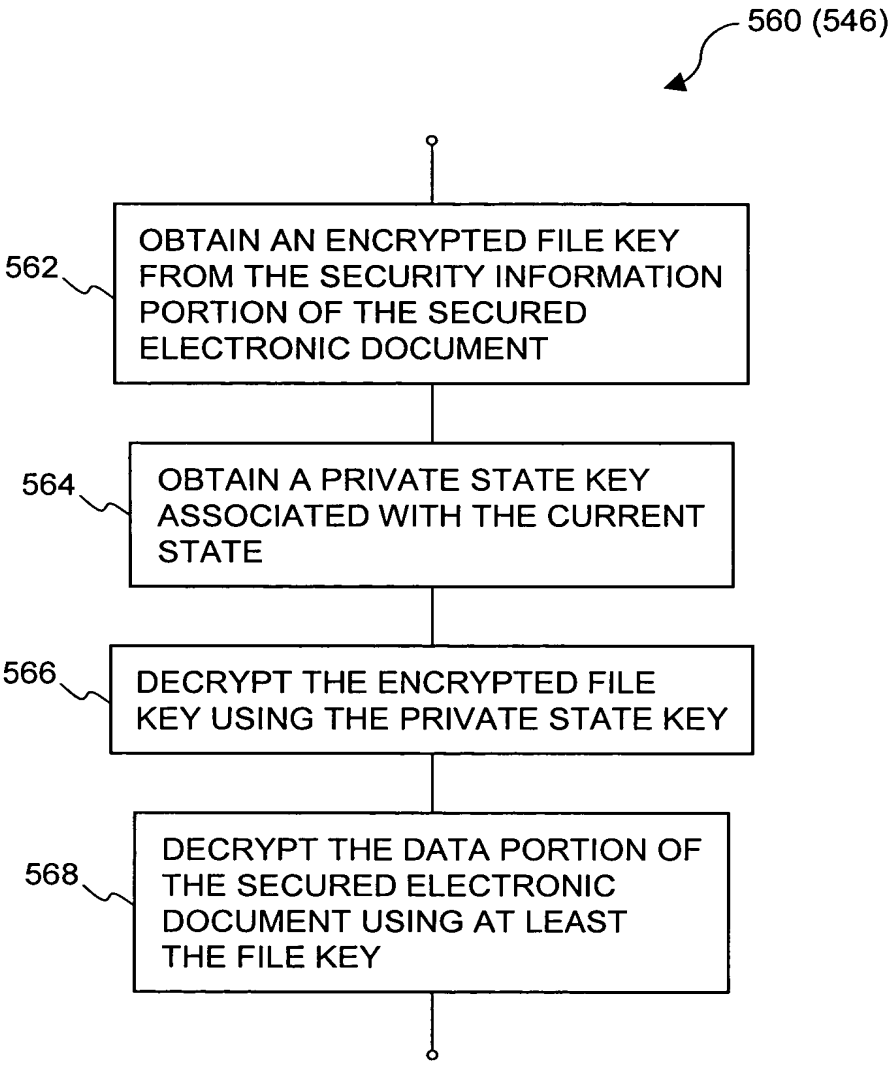
560 (546)
562
OBTAIN AN ENCRYPTED FILE KEY FROM THE SECURITY INFORMATION PORTION OF THE SECURED ELECTRONIC DOCUMENT
564
OBTAIN A PRIVATE STATE KEY ASSOCIATED WITH THE CURRENT STATE
566
DECRYPT THE ENCRYPTED FILE KEY USING THE PRIVATE STATE KEY
568
DECRYPT THE DATA PORTION OF THE SECURED ELECTRONIC DOCUMENT USING AT LEAST THE FILE KEY

FIG. 5D

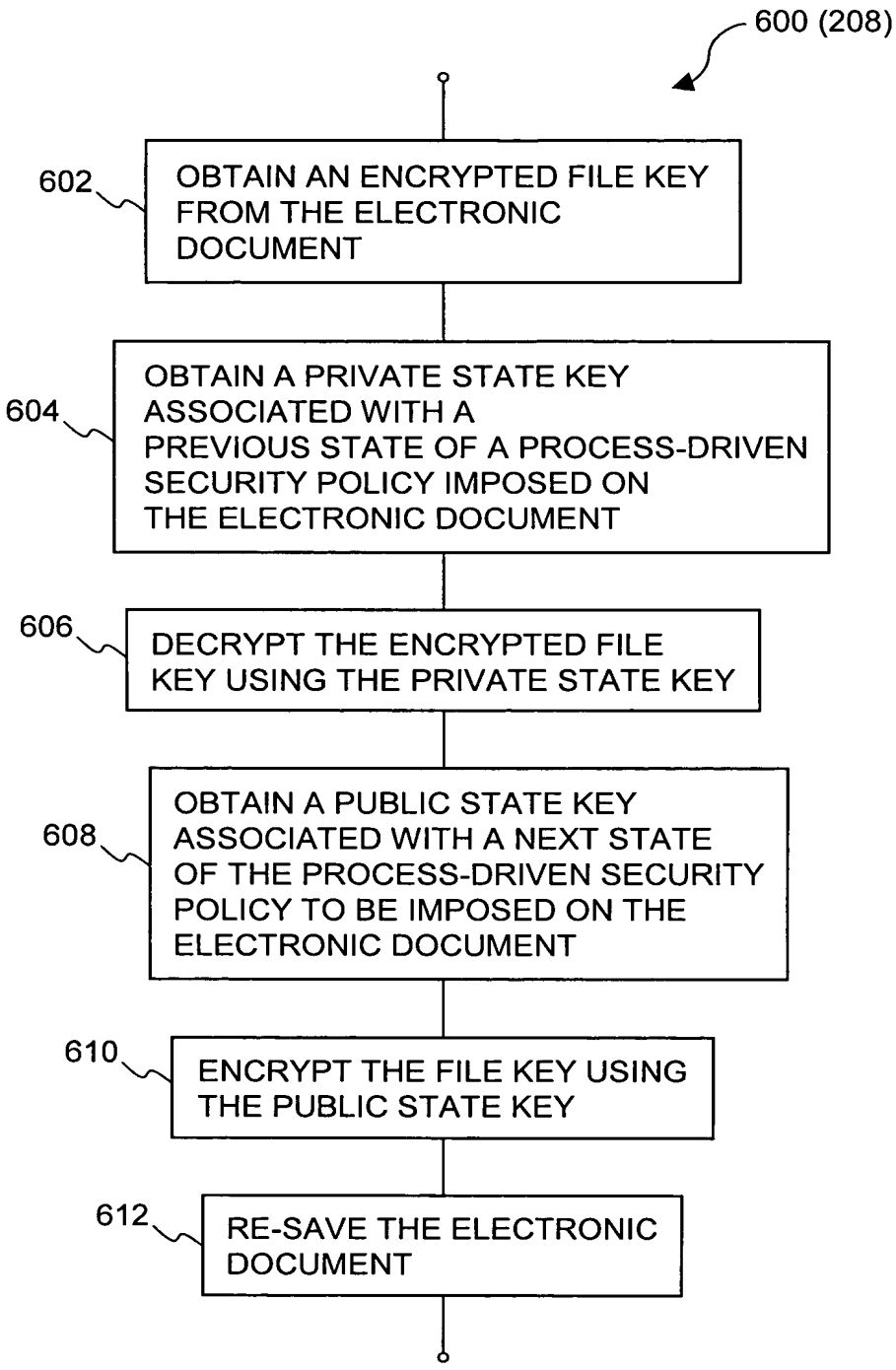
600 (208)
602
OBTAIN AN ENCRYPTED FILE KEY FROM THE ELECTRONIC DOCUMENT
604
OBTAIN A PRIVATE STATE KEY ASSOCIATED WITH A PREVIOUS STATE OF A PROCESS-DRIVEN SECURITY POLICY IMPOSED ON THE ELECTRONIC DOCUMENT
606
DECRYPT THE ENCRYPTED FILE KEY USING THE PRIVATE STATE KEY
608
OBTAIN A PUBLIC STATE KEY ASSOCIATED WITH A NEXT STATE OF THE PROCESS-DRIVEN SECURITY POLICY TO BE IMPOSED ON THE ELECTRONIC DOCUMENT
610
ENCRYPT THE FILE KEY USING THE PUBLIC STATE KEY
612
RE-SAVE THE ELECTRONIC DOCUMENT

*FIG. 6*

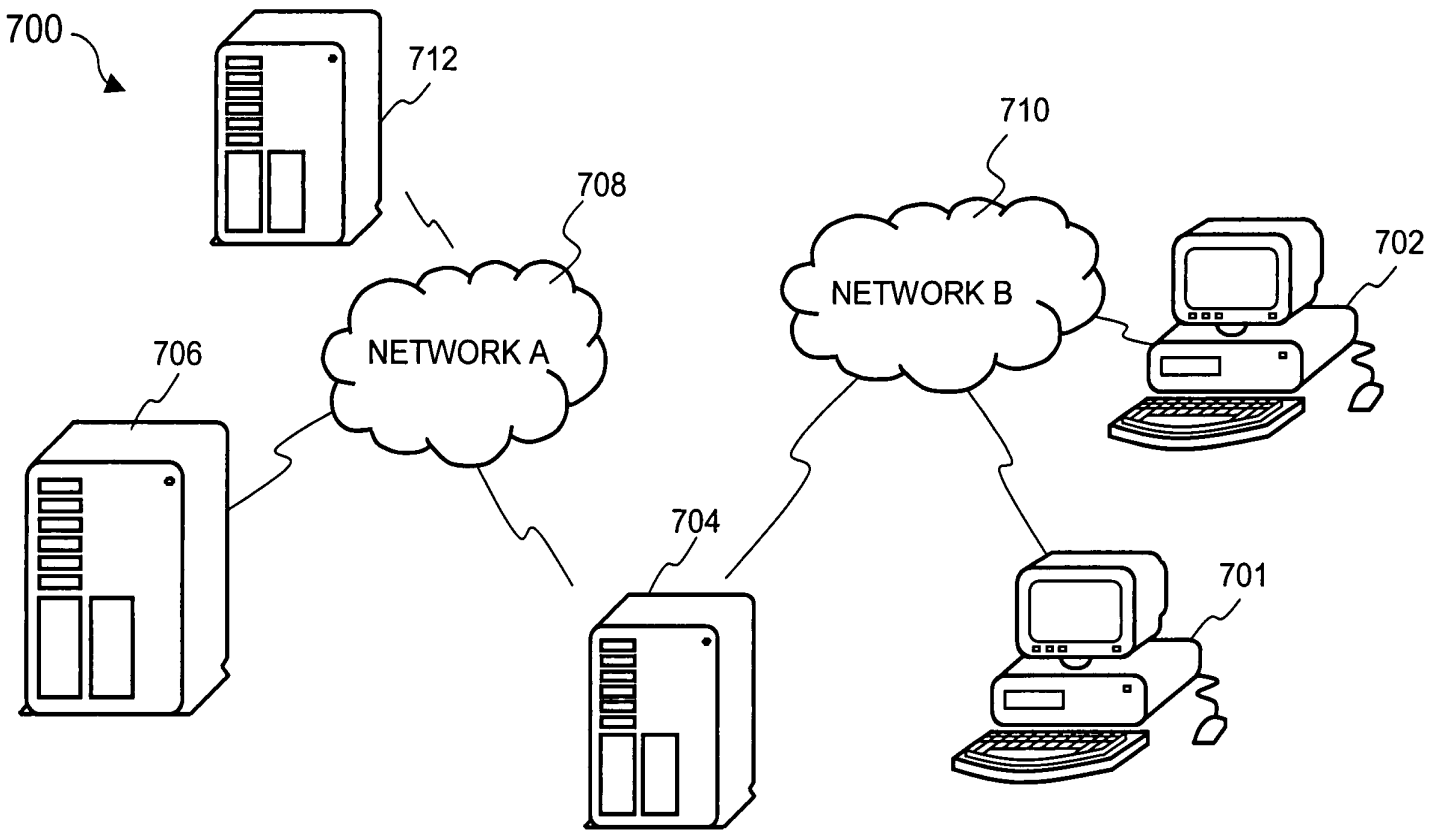


FIG. 7

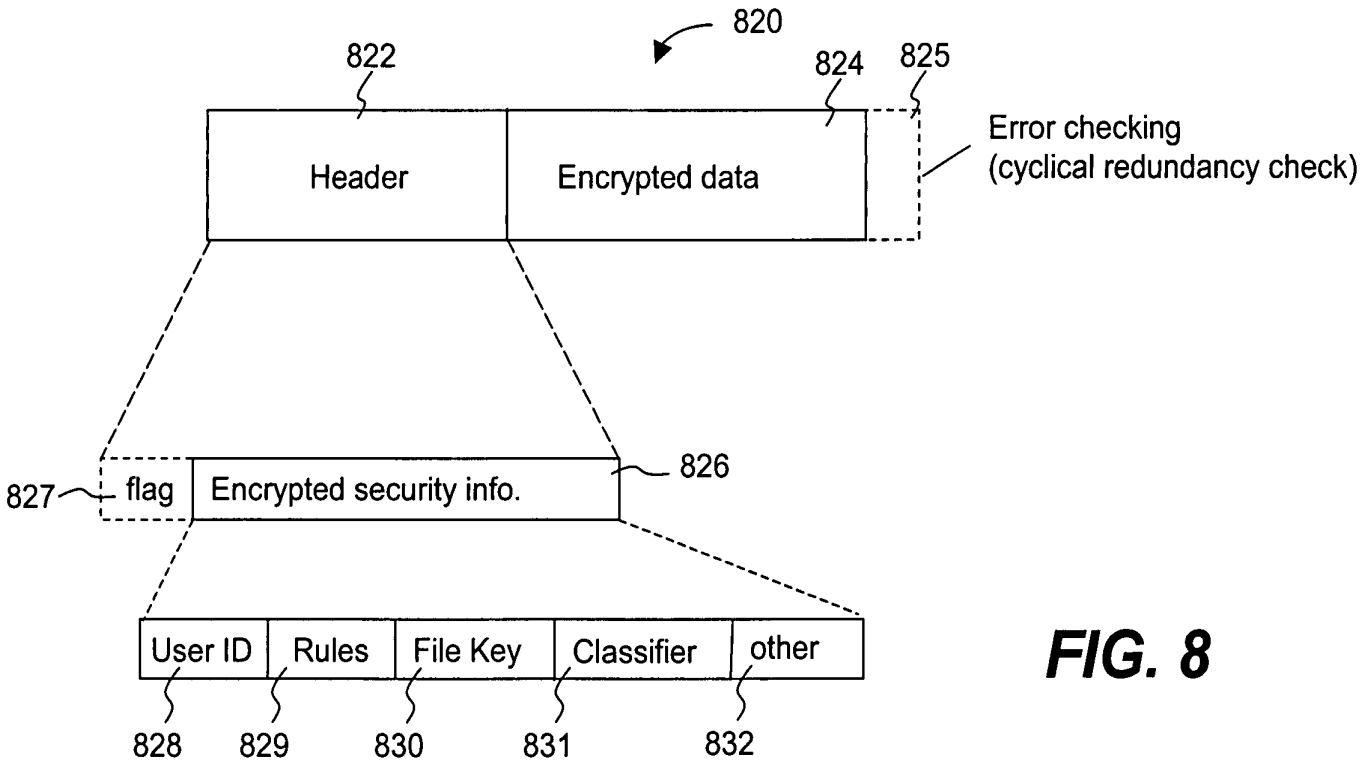
820
822
824
825
Header
Encrypted data
Error checking
(cyclical redundancy check)
827
flag
Encrypted security info.
826
User ID
Rules
File Key
Classifier
other
828
829
830
831
832

FIG. 8